(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－341327
（P2000－341327A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｇ	９Ａ００１
12/66			Ｂ	

審査請求　未請求　請求項の数42　ＯＬ　（全 24 頁）

(21)出願番号　特願平11－147663

(22)出願日　平成11年５月27日(1999.5.27)

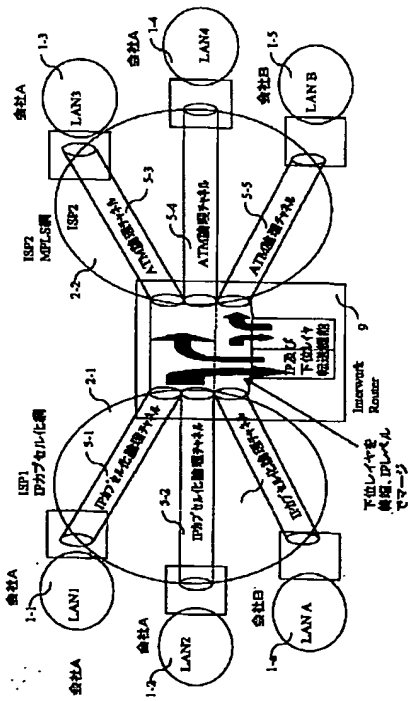
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　坂本　健一
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　星野　和義
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　ＶＰＮ構成方式、インターワークルータ装置、パケット通信方法、データ通信装置及びパケット中継装置

(57)【要約】
【課題】　複数インターネットサービスプロバイダ(ISP)にまたがる仮想専用網(VPN：Virtual Private Network)を提供することである。
【解決手段】　両インターネットサービスプロバイダのネットワーク接続部分のインターワークゲートウェーにおいて、各パケットの方路を決定する際に、VPNを構成するために導入されるカプセル化ヘッダの領域とIPヘッダ両方の領域の情報を用いて方路を決定し、更に出力側網におけるカプセル化ヘッダも前記情報から構成する。
【効果】　仮想専用線の相互接続が可能となり、複数インターネットサービスプロバイダにまたがるVPNを構成できる。また第一の網と第二の網のＱｏＳ情報をインターワークすることができる。

図1



【特許請求の範囲】

【請求項１】可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第一の通信網と前記第二の通信網の接続点では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第一の通信網で使用する第二のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるＶＰＮ（Virtual Private Network）構成方式。

【請求項２】可変長パケット通信方式にインターネットプロトコルを用いることを特徴とした請求項１に記載のＶＰＮ構成方式。

【請求項３】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項２記載のＶＰＮ構成方式。

【請求項４】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＡＴＭ通信方式のヘッダを使用することを特徴とした請求項２記載のＶＰＮ構成方式。

【請求項５】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＨＤＬＣ（ＰＰＰ、フレームリレー）通信方式のヘッダを使用することを特徴とした請求項２記載のＶＰＮ構成方式。

【請求項６】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＭＰＬＳ（Multi-Protocol Layer Switching）通信方式のヘッダを使用することを特徴とした請求項２記載のＶＰＮ構成方式。

【請求項７】可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供し、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、閉域網を構成することのできる複数の通信網があり、それぞれの接続点では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第一の通信網で使用する第二のカプセルヘッダを生成することにより２つの通信網にまたがる閉域網を構成することにより、複数網にまたがる閉域網を構成することを特徴とするＶＰＮ構成方式。

【請求項８】可変長パケット通信方式にインターネットプロトコルを用いることを特徴とした請求項７に記載のＶＰＮ構成方式。

【請求項９】それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項８記載のＶＰＮ構成方式。

【請求項１０】それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＡＴＭ通信方式のヘッダを使用することを特徴とした請求項８記載のＶＰＮ構成方式。

【請求項１１】それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＨＤＬＣ（ＰＰＰ、フレームリレー）通信方式のヘッダを使用することを特徴とした請求項８記載のＶＰＮ構成方式。

【請求項１２】それぞれの網で使用されるカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＭＰＬＳ（Multi-Protocol Layer Switching）通信方式のヘッダを使用することを特徴とした請求項８記載のＶＰＮ構成方式。

【請求項１３】それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、２つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報をパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラス

の領域にマッピングを行うことを特徴とする請求項１に記載のＶＰＮ構成方式。

【請求項１４】それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、２つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報をパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラスの領域にマッピングを行うことを特徴とする請求項８に記載のＶＰＮ構成方式。

【請求項１５】可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点には双方の網に所属するインターワークルータを配置し、

前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるＶＰＮ（Virtual Private Network）構成方式。

【請求項１６】可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二の網のインターワークルータ装置に転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の網から第一の網に送られるパケットに関しては、

第二の網の前記インターワークルータ装置では、第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるＶＰＮ（Virtual Private Network）構成方式。

【請求項１７】可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他の

ユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを可変長パケットを識別するＩＸを介して接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、ＩＸの通信網への方路選択及び前記インターワークカプセルヘッダを生成してＩＸに転送し、

ＩＸではインターワークカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第二のの通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二のインターワークルータに転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成してＩＸに転送し、

ＩＸではインターワークカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、

第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるＶＰＮ（Virtual Private Network）構成方式。

【請求項１８】可変長パケットにより通信を行うユーザ

に対してパケット通信サービスを提供するための第一の通信網と、

同様に可変長パケットにより通信を行うユーザに対してパケット通信サービスを提供するための第一の通信網があり、

前記第一の通信網では、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第一のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

前記第二の通信網でも同様に、特定のユーザのパケットを他のユーザのパケットと混合させない閉域網を構成するために、前記通信網の内部では可変長パケットに対して網内を転送するために特別に付与する第二のカプセルヘッダを網の入り口で付与し、網の出口で削除する構成を持ち、

双方の網の接続点は、それぞれインターワークルータを配置して前記両インターワークルータを可変長パケットを識別しないで下位レイヤにより転送を行うＩＸを介して接続する形式をとり、両インターワークルータ間では他網との接続を行う特定のユーザのパケットを他のユーザのパケットと分離するためにインターワークカプセルヘッダを使用して転送することとし、

第一の網から第二の網に送られるパケットに関しては、

第一の網の前記インターワークルータ装置では、第一の通信網から第二の通信網に転送される特定のユーザのパケットに対しては、第一のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、ＩＸの通信網への方路選択及び前記インターワークカプセルヘッダを生成してＩＸに転送し、

ＩＸではインターワークカプセルヘッダにより、第二のの通信網への方路選択及び前記インターワークカプセルヘッダを生成して第二のインターワークルータに転送し、

第二の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より第二の通信網への方路選択及び第二の通信網で使用する第二のカプセルヘッダを生成し、

第二の通信網から第一の通信網に転送される特定のユーザのパケットに対しては、第二のカプセルヘッダ及び可変長パケットのヘッダの組み合わせより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成してＩＸに転送し、

ＩＸではインターワークカプセルヘッダにより、第一の通信網への方路選択及び前記インターワークカプセルヘッダを生成して第一の網のインターワークルータ装置に転送し、

第一の網のインターワークルータ装置ではインターワークカプセルヘッダ及び可変長パケットのヘッダ情報より

第一の通信網への方路選択及び第一の通信網で使用する第一のカプセルヘッダを生成することにより、
第一の網及び第二の網にまたがる閉域網を構成することを特徴とする、可変長パケット通信によるＶＰＮ（Virtual Private Network）構成方式。

【請求項１９】複数のネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、
前記複数のネットワークのうち少なくとも２つのネットワークは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、
第一のカプセル化ネットワークからカプセル化された可変長パケットが到来し、第二のカプセル化ネットワークへパケットが転送される場合には、第一のネットワークにおけるカプセルヘッダと可変長パケットヘッダの組み合わせにより第二のネットワークへの出力伝送路及び第二のネットワーク内で使用されるカプセル化ヘッダを生成し、第一のネットワークで使用されるカプセル化ヘッダを削除し、第二のネットワークで使用されるカプセル化ヘッダを付与して第二のネットワークに出力することを特徴とするインターワークルータ装置。

【請求項２０】前記可変長パケットがインターネットプロトコルパケットであることを特徴とする請求項１９記載のインターワークルータ装置。

【請求項２１】前記第一のカプセル化ネットワークのカプセル化プロトコルと前記第二のカプセル化ネットワークのカプセル化プロトコルが異なるカプセル化プロトコルを採用していることを特徴とする請求項１９記載のインターワークルータ装置。

【請求項２２】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルによるカプセルヘッダを用いることを特徴とした請求項１９記載のインターワークルータ装置。

【請求項２３】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＡＴＭ通信方式のヘッダを使用することを特徴とした請求項１９記載のインターワークルータ装置。

【請求項２４】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＨＤＬＣ（ＰＰＰ、フレームリレー）通信方式のヘッダを使用することを特徴とした請求項１９記載のインターワークルータ装置。

【請求項２５】第一の網または第二の網のカプセル化ヘッダとして、インターネットプロトコルの下位レイヤにあたる、ＭＰＬＳ（Multi-Protocol Layer Switching）通信方式のヘッダを使用することを特徴とした請求項１９記載のインターワークルータ装置。

【請求項２６】それぞれの網において使用されるカプセル化ヘッダ内にパケット転送の優先度クラスを持ち、２つの網の接続点では、パケットが転送されてきた第一の網で使用されている前記カプセル化ヘッダ内の前記優先度クラスの情報をパケットが転送されていく第二の網で使用されている前記カプセル化ヘッダ内の優先度クラスの領域にマッピングを行うことを特徴とする請求項１９記載のインターワークルータ装置。

【請求項２７】前記各伝送路は下位レイヤ処理部に収容されパケットレイヤ処理部を介してコアスイッチと接続する構成を持ち、前記下位レイヤ処理部では到来した可変長パケットのカプセルヘッダの解析を行い、装置内部で使用する装置内入力ＶＰＮ番号をカプセルヘッダから生成し、装置内ＶＰＮ番号と可変長パケットをパケットレイヤ処理部に転送する機能を持ち、パケットレイヤ処理部では装置内入力ＶＰＮ番号と可変長パケットのヘッダ領域の情報から出力方路番号及び装置内出力カプセル番号を生成し、コアスイッチでは出力方路番号に応じて所望の伝送路に接続されるパケットレイヤ処理部を選択して装置内出力カプセル番号及びパケットレイヤ処理部を介してパケットを下位レイヤ処理部に転送し、下位レイヤ処理部では装置内出力カプセル番号より出力する網で使用するカプセルヘッダに変換することによりカプセル化を行うことを特徴とする請求項１９記載のインターワークルータ装置。

【請求項２８】前記装置内入力ＶＰＮ番号及び装置内出力ＶＰＮ番号にＱｏＳを識別するフィールドを設け、入力側の網のカプセル化ヘッダから前記入力ＶＰＮ番号のＱｏＳフィールドにマッピングを行い、前記パケットレイヤ処理部では入力ＶＰＮ番号のＱｏＳフィールドの値から出力側ＶＰＮ番号のＱｏＳフィールドにマッピングを行い、出力側下位レイヤ処理部では出力側ＶＰＮ番号のＱｏＳフィールドの値から出力側カプセル化ヘッダのＱｏＳに相当するフィールドにマッピングを行うことにより、第一のネットワークのＱｏＳ情報を第二のネットワークのＱｏＳ情報に伝達することを特徴とした請求項１９記載のインターワークルータ装置。

【請求項２９】第一のネットワークのカプセル化プロトコルにはＡＴＭヘッダを用い、第二のネットワークのカプセル化プロトコルにはＩＰカプセル化を用い、第一のネットワークから到来した可変長パケットのＡＴＭヘッダに付与されているＣＬＰビットの値を請求項２８に記載した方法で第二のネットワーク側のＩＰカプセルヘッダのＴＯＳフィールドにマッピングし、第二ネットワークから到来した可変長パケットのＩＰカプセルヘッダに付与されているＴＯＳの値を請求項２８に記載した方法で第一のネットワーク側のＡＴＭヘッダのＣＬＰフィールドにマッピングすることを特徴とする請求項２８記載のインターワークルータ装置。

【請求項３０】前記可変長パケットにはＩＰパケットを用い、入力するカプセル化プロトコルより固定長の入力ＶＰＮ番号を生成し、入力ＶＰＮ番号及びＩＰパケット

のヘッダ領域の組み合わせにより出力方路番号及び固定長の出力ＶＰＮ番号を生成し、出力側で前記ＶＰＮ番号からカプセル化ヘッダを生成することを特徴とする請求項１９記載のインターワークルータ装置。

【請求項３１】ひとつのネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、

前記ひとつのネットワークでは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、

カプセル化された可変長パケットが到来し、所望の方路にパケットが転送される場合には、入力側カプセルヘッダと可変長パケットヘッダの組み合わせにより出力側伝送路及び出力側で使用されるカプセル化ヘッダを生成し、入力側で使用されるカプセル化ヘッダを削除し、出力側で使用されるカプセル化ヘッダを付与して第二のネットワークに出力することを特徴とするインターワークルータ装置。

【請求項３２】複数のネットワークに接続される伝送路を収容し、各伝送路から到来する可変長パケットを所望のネットワークに出力する機能を持ち、

前記複数のネットワークのうち少なくとも２つのネットワークは、前記ネットワークの内部で使用するカプセルヘッダを用いて可変長パケットをカプセル化して転送を行うカプセル化ネットワークであり、

第一のカプセル化ネットワークからカプセル化された可変長パケットが到来し、第二のカプセル化ネットワークへパケットが転送される場合には、第一のネットワークにおけるカプセルヘッダと可変長パケットヘッダの組み合わせにより第二のネットワークへの出力伝送路及び第二のネットワーク内で使用されるカプセル化ヘッダを生成し、第一のネットワークで使用されるカプセル化ヘッダを削除し、第二のネットワークで使用されるカプセル化ヘッダを付与して第二のネットワークに出力することによりカプセル化プロトコルを変換する機能を持つことを特徴とするインターワークルータ装置。

【請求項３３】第１の通信網の入り口で、上記第１の通信網で閉域網を構成するために使用される第１のカプセルヘッダが付与された、宛先情報を含むヘッダを有するパケットを受信し、上記パケットを第２の通信網に送信するパケット通信方法であって、

上記第１のカプセルヘッダが付与された上記パケットを受信すると、上記ヘッダと上記第１のカプセルヘッダとから、上記第２の通信網で閉域網を構成するために使用される第２のカプセルヘッダを生成し、

上記第１のカプセルヘッダが付与された上記パケットから上記第１のカプセルヘッダを除去し、

上記パケットに上記第２のカプセルヘッダを付与することを特徴とするパケット通信方法。

【請求項３４】上記ヘッダと上記第１のカプセルヘッダとを用いて方路検索を行うことを特徴とする請求項３３に記載のパケット通信方法。

【請求項３５】第１の通信網の入り口で、上記第１の通信網で閉域網を構成するために使用される第１のカプセルヘッダが付与された、宛先情報を含むヘッダを有するパケットを受信し、上記パケットを第２の通信網に送信するパケット通信方法であって、　上記第１のカプセルヘッダが付与された上記パケットを受信すると、上記ヘッダと上記第１のカプセルヘッダとから、上記第２の通信網で閉域網を構成するために使用される第２のカプセルヘッダ生成するのに必要なインデックスを生成し、

上記第１のカプセルヘッダが付与された上記パケットから上記第１のカプセルヘッダを除去し、

上記第２のカプセルヘッダ生成するのに必要なインデックスに基づき上記パケットに上記第２のカプセルヘッダを付与することを特徴とするパケット通信方法。

【請求項３６】上記ヘッダと上記第２のカプセルヘッダ生成するのに必要なインデックスとを用いて方路検索を行うことを特徴とする請求項３５に記載のパケット通信方法。

【請求項３７】前記パケットは、ＩＰ（インターネットプロトコル）パケットであることを特徴とする請求項３３乃至請求項３６の何れかに記載のパケット通信方法。

【請求項３８】前記第１のカプセルヘッダ及び第２のカプセルヘッダは、インターネットプロトコルによるカプセルヘッダを用いることを特徴とする請求項３７に記載のパケット通信方法。

【請求項３９】その中で閉域網を構成するために、宛先情報を含むヘッダが付加されたデータに第１のカプセルヘッダを付与する第１の通信網と、その中で閉域網を構成するために、宛先情報を含むヘッダが付加されたデータに第２のカプセルヘッダを付与する第２の通信網とを相互に接続する通信装置であって、

上記第１の通信網から送信された上記第１のカプセルヘッダが付与されたデータを受信したとき、上記ヘッダと上記第１のカプセルヘッダとによりルート検索を行い、

上記ヘッダと上記第１のカプセルヘッダとから上記第２のカプセルヘッダを生成し、上記第１のカプセルヘッダを除去する一方で上記生成した第２のカプセルヘッダを付与する受信処理部と、

上記受信処理部に接続され、上記ルート検索の結果に応じた方路に、上記第２のカプセルヘッダが付与されたデータを送信するスイッチとを有することを特徴とする通信装置。

【請求項４０】上記スイッチに接続され、上記スイッチから上記第２のカプセルヘッダが付与されたデータが送信され、そのデータを上記第２の通信網に送信する送信処理部を有することを特徴とする請求項３９に記載の通信装置。

【請求項４１】その中で閉域網を構成するために、ＩＰ（Internet Protocol）パケットに第１のカプセルヘッダを付与して通信を行う第１の通信網と、その中で閉域網を構成するために、ＩＰパケットに第２のカプセルヘッダを付与して通信を行う第２の通信網とを相互に接続するパケット中継装置であって、

上記第１の通信網から送信された上記第１のカプセルヘッダが付与されたＩＰパケットを受信したとき、上記ＩＰパケット内のＩＰヘッダと上記第１のカプセルヘッダとにより上記第２のカプセルヘッダを生成するカプセルヘッダ生成手段と、

上記カプセルヘッダ作成手段と接続され、上記第１の通信網から送信された上記第１のカプセルヘッダが付与されたＩＰパケットを受信すると、上記第１のカプセルヘッダを除去すると共に上記第１のカプセルヘッダが除去されたＩＰパケットに上記カプセルヘッダ生成手段で生成された第２のカプセルヘッダを付加する手段とを有することを特徴とするパケット中継装置。

【請求項４２】上記カプセルヘッダ生成手段は、上記ＩＰパケット内のＩＰヘッダと上記第１のカプセルヘッダとによりインデックスを生成する手段と、上記インデックスを生成する手段で生成されたインデクスに応じて上記第２のカプセルヘッダを生成する手段とを有することを特徴とする請求項４１に記載のパケット中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はインターネットにおける仮想専用網（ＶＰＮ：Virtual Private Network）構築方法及びインターネットサービスプロバイダ間を接続するインターワークルータに関する。

【０００２】

【従来の技術】インターネット・プロトコル（Internet protocol: IP）ネットワーク上では、電子メール、ＷＷＷ（World Wide Web）などのアプリケーションを使用することができる。また、IPネットワークは、従来の電話ベースの交換網と比較して構築コストが安い。そのためインターネットは近年爆発的に普及している。このような状況の下、ＩＰで構築した企業内網（イントラネット）は、企業活動にも欠かすことの出来ないものとなってきている。

【０００３】企業は複数の地域に偏在している場合が多い。この場合、各地域の企業網を相互接続し、一つの企業網を構築する必要が生じる。企業網を複数地域にわたって構築する場合、次の２つの方法が考えられる。

【０００４】第１は、各地域の企業内網を専用線で相互接続することである。このように構築することにより、企業網を外部のネットワークから隔絶、セキュリティを確保を確保することができる。

【０００５】第２に、ＩＰｓｅｃ（IP security protocol）技術により、自網のネットワークのパケットを識別

する機能を端末に設け、インターネット内ではグローバルアドレスに基づくＩＰパケットとして転送を行うことである。悪意のユーザからの攻撃にはこの識別機能と、暗号化により対抗することでＶＰＮを実現することができる。

【０００６】しかし、専用線を使用するとネットワークコストが上昇してしまうこと、さらにＩＰｓｅｃ方式によるＶＰＮでは、アタック及び暗号解読により悪意のユーザの侵入を許したり、暗号化処理が高速ネットワークの速度のボトルネックになったり、端末コストが上昇するという問題があった。

【０００７】このため、インターネットが普及し、インターネットが廉価で使用できるようになるに従い、網が提供するＩＰの下位レイヤの機能を用い、インターネット上に仮想的に専用網を構築し、コストを押さえ、かつ外部のネットワークから隔絶した安全な、かつ何らかの品質保証行い要求が高まってきた。

【０００８】この要求を満たすネットワークとして次のようなＶＰＮが考えられている。ＶＰＮを提供するインターネット・サービス・プロバイダ（Internet Service Provider：ISP）のネットワークの入り口でカプセル化を行う。ISPのネットワーク上では、このカプセル化したヘッダに基づき転送を行い、ネットワークの出口でカプセルヘッダを外す。このＶＰＮ構成方式では、ＶＰＮ固有のカプセル化ヘッダを用いることにより外部のネットワークから隔絶し、セキュリティを確保している。また、このカプセル化の具体的なプロトコルとしては、ＩＰカプセル化、ＭＰＯＡ（Multi Protocol over ATM）、ＭＰＬＳ（Multi Protocol Layer Switching）等の方式があり、１９９９年２月現在、ITU-T SG13やIETFなどの標準化団体で検討が行われている。また、ITU-T SG13では、網の内部をE.164アドレスによりカプセル化して転送する、Core Protocol(別称GMN-CL)についての検討も行われている。

【０００９】NTT R&D vol.47 No.4 1998（平成10年4月10日発行）は、GMN-CLにおけるユーザ網とコア網のインターワークを行うアクセス系・エッジノードの構成法を提案している。

【００１０】

【発明が解決しようとする課題】近年の企業活動は広範囲に渡っている。このため、例えば、日、米、欧に拠点を持ち、それぞれの拠点でイントラネットを構築した上で、ＶＰＮにより、それらを相互接続したいというニーズが生じてくるものと考えられる。

【００１１】他方、ISPはある特定の地域でサービスを提供しているのが一般的なため、前記したような各拠点のネットワークをＶＰＮにより接続するためには、複数のISPをまたがった形でＶＰＮを構築する必要がある。

【００１２】なお、複数のISPを相互に接続する場合、インターワークのためのゲートウェーを設け、相互接続

を行う。このインターワークルータでは、双方のネットワークから到来した相手網行きのパケットをＩＰヘッダに従って相手網に転送することで、インターワークを実現する。また、日経コミュニケーション1997年12月15日号146頁に記されているように、複数ネットワークの相互インターワークのために、IX（Internet Exchange）と呼ばれる装置を用いて互いのネットワークを接続し、このIXにより、互いの網間で転送されるパケットの転送を行っても良い。このようなIXには、IPパケットを識別して転送を行う「レイヤ３フォワーディング」や、ATM通信装置などで、下位レイヤのヘッダを識別して転送を行う「レイヤ２フォワーディング」を用いる方式がある。

【００１３】本願発明者等は、複数のISPのネットワークをまたがる形でＶＰＮを構成しようとした場合の問題点を検討した。まず、各インターネットサービスプロバイダのネットワークでＶＰＮを構築するために、各ネットワーク内でそれぞれカプセル化を行う。各ネットワークのカプセル化プロトコルは、一般に異なるものとなると考えられる。この場合、インターワークルータでは、双方のネットワークの共通のプロトコルであるＩＰパケットのＩＰヘッダ情報を検索して宛先方路を決定し、他網行きのパケットであるか否かを検索する必要がある。

【００１４】しかし、インターワークルータは、ＩＰレイヤより下位レイヤのプロトコルはインターフェースで終端してしまうため、前段の網でＶＰＮを構成するためにつけられているカプセル化ヘッダをはずしてＩＰアドレスを検索する事により次のホップ情報を決定し、また後段の網でのＶＰＮを構成するためのカプセルヘッダを生成してパケットに付与することになる。したがって、インターワーク装置内部では、ＶＰＮ内のパケットとＶＰＮ以外の網のパケットとが混在してしまう。そのため、悪意のユーザによる不正ヘッダの付与により、インターワークルータを基点としてＶＰＮへの侵入が可能になるという問題がある。

【００１５】また、企業によってはグローバルアドレスを使用せずにインターナルアドレスを用いてＶＰＮを構成することがある。この場合、インターワークルータでカプセル化ヘッダを一旦はずしてしまうと、受信側のＩＳＰ側では、インターナルアドレスが複数のＶＰＮでそれぞれ独自に使用されているので、同一のアドレスを持つパケットを区別することが出来ない。このため、パケットの転送先が決定できない。複数のＩＳＰにまたがって、インターネット上にＶＰＮ構成する場合、上述のような問題点がある（第１の課題）。

【００１６】更にそれぞれのＩＳＰにおけるサービスは均一でない。例えば通信品質を例に説明すると、あるＩＳＰではＡＴＭのＶＣを用いてパスを張ることにより各ＶＰＮの品質の保証しており、別のＩＳＰではＤｉｆｆｓｅｒｖ（Ｄｉｆｆｅｒｅｎｃｉａｔｅｄ Ｓｅｒｖｉｃｅｓ）により品質の保証を行っている場合、双方で構成するＶＰＮを相互に接続する場合、エンド・トゥー・エンドで通信品質を規定することは困難である。（第２の課題）。

【００１７】上述のように、実用レベルで、複数のＩＳＰにまたがってインターネット上にＶＰＮを構築することは困難である。

【００１８】そこで、本発明は複数のＩＳＰにまたがってＶＰＮ構築する方法及び、複数のＩＳＰにまたがってＶＰＮ構築する場合において、それらのＩＳＰ間を接続するインターワークルータを提供することにある。

【００１９】

【課題を解決するための手段】第１の課題を解決するため、ＶＰＮ識別番号であるカプセル化ヘッダとIPヘッダ双方の情報を用いて、出力方路の決定及び出力側ＩＳＰ網内でのカプセル化ヘッダの生成を行う機能をインターワークルータ装置に設ける。下位レイヤにＡＴＭを用いるＭＰＬＳ網を運用するＩＳＰ同士を接続する場合を例により具体的に説明すると、ＶＰＮ識別に使用するカプセル化ヘッダであるＡＴＭのＶＰＩ、ＶＣＩ等のヘッダ情報と、ＩＰアドレスをキーに検索を行い、次の方路及び次のネットワーク内部でのＶＰＮ識別に使用するＡＴＭのＶＰＩ，ＶＣＩ等のヘッダ情報を生成し、後段の網に送り出す際に生成したヘッダ情報を付与して送出する。

【００２０】これによりＶＰＮのインターワークが実現でき、複数のＩＳＰにまたがる地域に対する、インターネット上でのＶＰＮ構成を構成することが出来る。

【００２１】第二の課題を解決するするために、入力側のカプセル化ヘッダ領域のＱｏＳをあらわすフィールドの値を、出力側のカプセル化ヘッダ領域のＱｏＳをあらわすフィールドの値にマッピングを行う。これにより、双方の網の品質情報を透過的に転送することができる。

【００２２】

【発明の実施の形態】以下、図を用いて本発明の実施例について説明する。

【００２３】図１、図２を用いて本発明による複数ＩＳＰにまたがる下位レイヤにより分離されたＶＰＮの構成法およびそのインターワークルータの役割について説明する。ここで下位レイヤとは、ＩＰパケットをカプセル化するプロトコルを指し、ＩＰパケットをＩＰヘッダでカプセル化する場合にも、このカプセルヘッダを下位レイヤのヘッダとして表記することとする。

【００２４】まず、図２により、従来のルータを用いて複数のＩＳＰにまたがるＶＰＮを構成した場合の問題点について説明する。図２では、下位レイヤでカプセル化することによりＶＰＮを実現するＩＳＰ１（２－１）とＩＳＰ２（２－２）が既存ルータ（９）によりインターワークしている。ＩＳＰ１はＡ地区でサービスを展開しており、ＬＡＮ１（１－１）、ＬＡＮ２（１－２）、Ｌ

ANａ（１－ａ）を収容している。ＩＳＰ２はＢ地区でサービスを展開しており、ＬＡＮ３（１－３）、ＬＡＮ４（１－４）、ＬＡＮｂ（１－ｂ）を収容している。また、ＬＡＮ１、ＬＡＮ２、ＬＡＮ３、ＬＡＮ４は同一会社のＬＡＮであり、ＶＰＮを構成したいと考えている。またＬＡＮａ、ＬＡＮｂも同一会社のＬＡＮであり、ＶＰＮを構成したいと考えている。このような場合、同一ＩＳＰ内においては、網の入り口と網の入り口にカプセルチャネルを張ることにより、他のユーザのパケットと分離することができるため、セキュリティの高いネットワークを構築できる。しかし、ＩＳＰ１とＩＳＰ２にわたってＶＰＮを設定しようとする場合、既存ルータでは入力側のインターフェース部で下位レイヤを終端し、IPレベルでマージしてからパケットフォワーでリング処理を行うため、ＩＰレベルで複数のユーザのパケットが混じってしまう問題がある。すなわち、ＶＰＮ内のパケットとそれ以外のパケットが混じってしまう。従って、悪意のユーザがＩＰアドレスを偽って網に侵入することも可能となる。さらに二つの会社がプライベートアドレスを用いて社内ＬＡＮを構築しようとした場合には、それぞれの会社では独立にアドレスをアサインするため、同一のＩＰアドレスをアサインすることがある。この場合、既存ルータではアドレスのバッティングのため、正しくパケットを転送することができない。

【００２５】次に図１を用いて、本発明による前記問題の解決法について説明する。例えば会社ＡのＬＡＮ１から会社ＡのＬＡＮ３に通信する場合を説明する。本実施例ではＩＳＰ１はＩＰカプセル化によりＶＰＮを実現しており、ＩＳＰ２はＭＰＬＳ（ＡＴＭによる）によりカプセル化を行いＶＰＮを実現している。ＬＡＮ１から到来したパケットはＩＳＰ１（２－１）に入るとＩＳＰ１はＩＰカプセル化を行い、パケットはＩＰカプセル化論理チャネル（５－１）通じてインターワークルータに到着する。インターワークルータ（９）ではパケットが搭載されてきたＩＰカプセル化論理チャネルを示すＩＰカプセル化ヘッダと、元々のパケットヘッダの双方から出力方路を検索すると共に、ＩＳＰ２内でのカプセル化ヘッダを作成する。本実施例ではＩＳＰ２はＭＰＬＳでサービスを行っているので、ＡＴＭのヘッダを作成する。ＡＴＭによりカプセル化されたパケットは、ＡＴＭ論理チャネル（５－３）を通り、ＬＡＮ３に送られる。インターワークルータでは、カプセルヘッダ及びＩＰヘッダで検索を行っているので、会社Ａと会社Ｂがそれぞれプライベートアドレスを用いて、ＩＰアドレスがバッティングする場合にもそれぞれ正しいあて先に転送することが可能となる。

【００２６】本実施例ではカプセル化プロトコルとして、ＩＰレイヤのカプセル化方式であるＩＰカプセル化と、ＡＴＭを用いてカプセル化を行う方式説明した。もちろんフレームリレーやＨＤＬＣ系のプロトコルを用いてカプセル化を行ってもよい。

【００２７】図３では本発明による、複数ＩＳＰにまたがるＶＰＮ構成法の１実施例について、網構成とプロトコルスタックを用いて説明する。ここではカプセル化プロトコルは限定していない。ＩＳＰ１（２－１）はエッジノード（３－１，３－２）を介してそれぞれＬＡＮ１（１－１）、ＬＡＮ２（１－２）を収容している。同様にＩＳＰ２（２－２）はエッジノード（３－３，３－４）を介してそれぞれＬＡＮ３（１－３）、ＬＡＮ４（１－４）をはじめとする複数の網を収容している。またそれぞれのＩＳＰは自網の入り口から出口にかけて、ＩＰパケットを網内で使用するヘッダでカプセル化して転送を行っている。そしてカプセルヘッダをＶＰＮに固有に割り当てることにより、ＶＰＮトラフィックを網内の別のトラフィックから識別してＶＰＮに関する閉域網を構成している。ＩＳＰ１（２－１）とＩＳＰ２（２－２）はインターワークルータ（１０）により互いにインターワークしており、相手網行きのトラフィックはインターワークルータを介して相手網に転送される。

【００２８】例えばＬＡＮ１とＬＡＮ３を結ぶＶＰＮ（ＶＰＮ１と呼ぶ事とする）を構成する場合について説明すると、ＬＡＮ１から送出されたＬＡＮ３宛のＩＰパケットはエッジノード（３－１）においてＩＰアドレスにより検索され、まずＶＰＮ１に属すインターワークルータ宛のパケットと認識され、ＶＰＮ１のインターワークルータ（１０）行きのカプセルヘッダ（レイヤ図中１０３ａ）が付与され、インターワークルータ（１０）に到達する。インターワークルータ（１０）はカプセルヘッダ（レイヤ図中１０３ａ）とＩＰアドレスにより検索され、ＶＰＮ１に属すエッジノード（３－３）宛のパケットであることを検索し、ＩＳＰ２内でＶＰＮ１でエッジノード（３－３）宛のカプセルヘッダ（レイヤ図中１０３ｂ）を付与し、ＩＳＰ２内をカプセルヘッダに従いエッジノード（３－３）に転送される。エッジノード（３－３）ではカプセルヘッダを外し、ＬＡＮ３にＩＰパケットを転送する。これにより、両網内にまたがるＶＰＮのＩＰパケットを他トラフィックと混合されることなくを転送することが出来る。

【００２９】なお、グローバルアドレスを用いたＩＰパケットについては、下位レイヤ情報に依存させず、ひとまとめにして転送先および（カプセルヘッダを使用する場合には）カプセルヘッダを決定することにより、従来の網内と同様に転送を行うことが出きる。

【００３０】インターワークルータ（１０）の動作を図４、図５、図６を用いて説明する。図４は従来のルータ装置の処理フローであり、図５、図６は本発明によるインターワークルータ（１０）の処理フローである。従来のルータでは、パケットが到着すると、ＩＳＰ１（２－１）での転送に用いられる物理レイヤを終端（２０１）し、ＩＳＰ１内の転送に使用したカプセルヘッダを除去

（２０２）してから、ＩＰヘッダの値により方路検索を行い（２０３）、スイッチを介して所望方路に転送する（２０４）。その後、ＩＳＰ２での転送に用いられるカプセルヘッダを付与（２０５）し、その後物理レイヤの処理を行って（２０６）伝送路から送出する。このフローでは、ＩＳＰ１のカプセルヘッダを除去して、ＩＰヘッダのみで方路を決定するため、複数ＶＰＮのトラフィックが一旦マージされてしまう。本発明のインターワークルータによれば、そのような問題を回避できる。

【００３１】図３は、本発明のインターワークルータ（１０）が実行するアルゴリズムであるパケットが到着すると、ＩＳＰ１（２－１）での転送に用いられる物理レイヤを終端（２１１）し、ＩＳＰ１内の転送に使用したカプセルヘッダとＩＰヘッダの値により方路検索およびＩＳＰ２内のカプセル化ヘッダの生成を行う（２１２）。その後ＩＳＰ１カプセルヘッダを除去（２１３）し、ＩＳＰ２での転送に用いられるカプセルヘッダを付与（２１４）し、スイッチに送信する。そして、スイッチにより、所望の方路に転送（２１５）される。その後物理レイヤの処理を行って（２１６）伝送路から送出する。これにより、別の網のトラフィックと分離することができる。また、スイッチに、カプセルヘッダが除去された裸のＩＰパケットが流れることがないので、この部分から他人がＶＰＮに挿入することは出来ない。すなわち、ＩＳＰ２内で使用される内部ヘッダが付加されていないＩＰパケットが紛れ込み、そのパケットがＩＳＰ２内のＶＰＮに流れ込むということはない。従って、安全性も高くなる。

【００３２】また別の実施例として図６を説明する。本実施例のインターワークルータは、ＩＳＰ１内の転送に使用したカプセルヘッダとＩＰヘッダの値の組と、カプセルヘッダインデックスとの対応テーブルと、カプセルヘッダインデックスとＩＳＰ２内の転送に使用したカプセルヘッダとの対応テーブルを有している。パケットが到着すると、ＩＳＰ１（２－１）での転送に用いられる物理レイヤを終端（２２１）し、ＩＳＰ１内の転送に使用したカプセルヘッダとＩＰヘッダの値により方路検索とカプセルヘッダインデックスの生成を行う（２２２）。その後、上記ＩＰパケットＩＳＰ１カプセルヘッダを除去（２２３）し、その除去されたＩＰパケットに、生成したカプセルヘッダインデックスを付与してスイッチに送信し、スイッチにより所望の方路に転送される（２２４）。そして、カプセルヘッダIndexからＩＳＰ２での転送に用いられるカプセルヘッダを生成、付与（２２５）する。その後物理レイヤの処理を行って（２２６）伝送路から送出する。この構成によっても、図５の場合と同様に、安全性の高い閉域網を構成することが出来る。すなわち、カプセルヘッダIndexが付与されていないＩＰパケットが紛れ込むことはない。

【００３３】次に図７～図１０を用いて、ＭＰＬＳによりＶＰＮをサポートするＩＳＰ１とＩＰカプセルを用いてＶＰＮをサポートするＩＳＰ２にまたがるＶＰＮの実現方式とパケット構成例を説明する。

【００３４】図７は網構成とプロトコルスタックを示している。図３ではカプセル化方式を特定せずに説明したが、図７は、ＩＳＰ１はＭＰＬＳ、ＩＳＰ２はＩＰカプセル化を採用した場合の例を示している。インターワークルータ（１０）では、図３と同様にカプセル化ヘッダに相当するＡＴＭレイヤ（１０４ａ）及びＩＰレイヤ（１０１）、ＩＰカプセルレイヤ（１０４ｂ）及びＩＰレイヤ（１０１）の組み合わせによりフォワーディングを行う。これにより、ＶＰＮがそれぞれプライベートアドレスを用いるためアドレスが重複する場合であっても、正しくフォワーディングすることが可能となる。

【００３５】図８により、ＩＰパケットをＡＴＭでカプセル化する方式を説明する。本カプセル化はＩＥＴＦのＲＦＣ１４８３で標準化されている方式である。ＩＰヘッダ（２５０）及びＩＰペイロード（２５１）からなるＩＰパケットにＬＬＣ／ＳＮＡＰ（２５３）を付与し、ＡＡＬ５ヘッダ（２５２）及びＡＡＬ５トレイラ（２５５）を付与してＡＡＬ５フレームを構成する。ＰＡＤ（２５４）はＡＡＬ５フレームをＡＴＭセルのペイロード（２５７）長である４８オクテットの定数倍にするために挿入する。そしてこのＡＡＬ５トレイラを４８オクテット毎に分割し、ＡＴＭヘッダ（２５６）を付与し、１乃至複数のＡＴＭセルとして転送を行う。

【００３６】図９はＲＦＣ７９１で示されるＩＰｖ４パケットフォーマットを示している。ＩＰカプセル化を行う際、カプセル化を行うプロトコルはＩＰｖ４ヘッダをそのまま使用し、網内のルータは既存のＩＰｖ４ルータを使用することができる。

【００３７】図１０はＩＰトンネルによるカプセル化方式を示している。ユーザの送信したＩＰヘッダ（２６０）及びＩＰペイロード（２６１）から構成されるＩＰパケットをカプセル化ヘッダ（２６４）でカプセル化しており、このカプセル化ヘッダはＩＰヘッダ（２６２）とトンネルヘッダ（２６３）から構成される。このカプセル化ヘッダはＩＳＰ２内で用いられるもので、網内で一意に識別が可能である。したがって、ユーザがプライベートアドレスを用いた場合でも、網内ではカプセルヘッダによりルーティングを行い、パケットを所望のエッジまで運ぶことができる。本例ではＲＦＣ１５８３によるトンネルヘッダの例を示したが、他にＩＰカプセル化にはＧＲＥカプセル化（ＲＦＣ１７９２）やＩＰモバイルなどがある。

【００３８】インターワークルータ（１０）では、図８や図１０で示したカプセルヘッダとユーザのＩＰアドレスを組み合わせてフォワーディング処理を行うことにより、安全なＶＰＮをＩＳＰにまたがり構成することができ、さらにユーザはプライベートアドレスを用いてＶＰ

Ｎを構築することができる。

【００３９】図１１乃至図１９を用いて、インターワークルータ（１０）の一実施例について説明する。

【００４０】図１１はインターワークルータ（１０）の１構成例である。制御部（５０）は装置全体の制御及び他ノードとのルーティング処理などを行っている。コアスイッチ（５１）は各パケットレイヤ処理部（５２）間のパケットの転送を行うスイッチである。下位レイヤ処理部（ＡＴＭ）（５３）はＩＳＰ１のＭＰＬＳ網を収容するインターフェースであり、下位レイヤ処理部（ＩＰカプセル）（５４）はＩＳＰ２のＩＰカプセル網を収容するインターフェースである。パケットレイヤ処理部（５２）は下位レイヤ処理部（５３，５４）から下位レイヤの情報及びＩＰパケットを受け取り、下位レイヤの情報とＩＰパケットのヘッダ情報の組み合わせによりパケットの転送先を決定する。

【００４１】まず受信方向の処理の流れから説明する。図１２に下位レイヤ処理部（ＡＴＭ）（５３）のブロック構成を示す。ＩＳＰ１の網から到来した信号はまず物理レイヤ処理部（１５０）にて物理レイヤを終端し、ＡＴＭレイヤ処理部（１５１）にてＡＴＭレイヤを終端する。この際、再構成されたＩＰパケットとともに、受信側のＶＰＮ識別機能を果たしているＡＴＭヘッダも同時にＶＰＮ番号付与部（１５２）に送付する。ＶＰＮ番号付与部（１５２）では装置内でＶＰＮの識別に利用するＶＰＮ番号をＡＴＭヘッダより生成する。この際受信側ＶＰＮ番号テーブル（１５３）が用いられる。そしてこのＶＰＮ番号とＩＰパケットはパケット処理部ＩＦ（１５４）を介してパケットレイヤ処理部に転送される。

【００４２】図１３には受信側ＶＰＮ番号テーブル（１５３）の構成例を示している。このテーブルでは入力側ＡＴＭヘッダ（３００）と入力側ＶＰＮ番号（３０３）のペアから構成されており、入力側ＡＴＭヘッダが入力キーとなって入力側ＶＰＮ番号（３０３）を出力する。入力キーとなる入力側ＡＴＭヘッダとしては、ＶＰＩ／ＶＣＩ（３０１）の他、パケットの転送優先度を示すＣＬＰ（Cell of Priority）ビット（３０２）をキーとしてもよい。そして装置内で汎用的に使用される入力側ＶＰＮ番号は装置内ＶＰＮ番号（３０４）の他にＱｏＳ（Quality of Service）を示すフィールド（３０５）を設けてもよい。またＣＬＰとＱｏＳのマッピングを行うテーブルをＶＰＮ識別のための本テーブルと独立に設けてもよい。

【００４３】図１４に下位レイヤ処理部（ＩＰカプセル）（５４）の実施例を示す。ＩＳＰ２から到来した信号は物理レイヤ処理部（１７０）にて物理レイヤを終端し、次にカプセルレイヤ受信処理部（１７１）にてカプセルヘッダの終端を行う。この際終端したカプセルヘッダをＩＰパケットと共にＶＰＮ番号付与部（１７２）へ送付する。ＶＰＮ番号付与部（１７２）では装置内でＶＰＮの識別に利用するＶＰＮ番号をＡＴＭヘッダより生成する。この際受信側ＶＰＮ番号テーブル（１７３）が用いられる。そしてこのＶＰＮ番号とＩＰパケットはパケット処理部ＩＦ（１５４）を介してパケットレイヤ処理部に転送される。

【００４４】図１５には受信側ＶＰＮ番号テーブル（１７３）の構成例を示している。このテーブルは、入力側カプセルヘッダ（３１０）と入力側ＶＰＮ番号（３０３）のペアから構成されており、入力側ＡＴＭヘッダが入力キーとなって入力側ＶＰＮ番号（３０３）を出力する。入力キーとなる入力側ＩＰカプセルヘッダとしては、カプセルヘッダのソースアドレス（３１１）の他、パケットの転送優先度を示すＴＯＳ（Type of Service）フィールド（３０２）をキーとしてもよい。そして装置内で汎用的に使用される入力側ＶＰＮ番号は装置内ＶＰＮ番号（３０４）の他にＱｏＳを示すフィールド（３０５）を設けてもよい。

【００４５】またＴｏＳとＱｏＳのマッピングを行うテーブルをＶＰＮ識別のための本テーブルと独立に設けてもよい。

【００４６】図１２から図１５を用いて説明した方式により、入力側ＶＰＮ番号（３０３）とＩＰパケットがパケットレイヤ処理部（５２）に到達した際の処理を図１６を用いて説明する。下位レイヤ処理部（１８０）を介して入力側ＶＰＮ番号（３０４）とＩＰパケットをルート検索・ＶＰＮ処理部（１８１）が受け取ると、ここではルート検索・ＶＰＮテーブル（１８２）を用いてＩＰヘッダ及び入力側ＶＰＮ番号の双方をキーにしてルート検索及び出力側ＶＰＮ番号を決定する。これにより出力方路及び出力側ＶＰＮ番号とＩＰパケットは、コアスイッチＩＦを介してコアスイッチに送付され、所望のパケットレイヤ処理部に到達することとなる。

【００４７】図１７にルート検索・ＶＰＮテーブルの構成例を示す。入力キーとして入力側ＶＰＮ番号（３２０）及びＩＰヘッダ（３２３）を用いて検索を行い、出力方路番号（３２５）及び出力側カプセル番号（３２６）を出力させる。出力方路番号（３２６）はコアスイッチ及びその他でパケットを所望のインターフェースに転送するための装置内識別子であり、出力側カプセル番号（３２６）は出力側の下位レイヤ処理部にてカプセルヘッダを付与するためのカプセルヘッダへの装置内識別子である。出力側カプセル番号（３２６）にはカプセル番号（３２７）の他にＱｏＳ（３２８）を設け、優先制御を行ってもよい。

【００４８】次に送信方向の処理について説明する。図１６を用いてパケットレイヤ処理部（５２）の処理例を示す。コアスイッチＩＦ（１８４）を介して出力側カプセル番号（３２６）及びＩＰパケットを受け取ると、これらの情報を下位レイヤ処理部ＩＦを介して下位レイヤ処理部（５３、５４）に転送する。

【００４９】図１２を用いて、下位レイヤ処理部（ＡＴＭ）（５３）の動作を説明する。下位レイヤ処理部（ＡＴＭ）（５３）ではパケットレイヤ処理部（５２）からパケットレイヤ処理部ＩＦ（１５９）を介して出力側カプセル番号（３２６）及びＩＰパケットを受信する。次にＡＴＭヘッダ決定部（１５７）はヘッダ生成テーブル（１５８）を用いてカプセルヘッダに対応するＡＴＭヘッダを出力側カプセル番号（３２６）から生成する。こうして生成されたＡＴＭヘッダとＩＰパケットはＡＴＭレイヤ送信処理部（１５６）でＡＴＭセルに変形され、物理レイヤ送信処理部（１５５）を介してＩＳＰ１のネットワークへと送信される。

【００５０】図１８にヘッダ生成テーブルの構成を示す。出力側カプセル番号をキーとして出力側ＡＴＭヘッダを出力する構成となっている。これにより出力側カプセル番号より出力側ＡＴＭヘッダを得ることができる。

【００５１】同様に図１４を用いて下位レイヤ処理部（ＩＰカプセル）（５４）の動作を説明する。下位レイヤ処理部（ＩＰカプセル）（５４）ではパケットレイヤ処理部（５２）からパケットレイヤ処理部ＩＦ（１５９）を介して出力側カプセル番号（３２６）及びＩＰパケットを受信する。次にカプセルヘッダ決定部（１７７）はヘッダ生成テーブル（１７８）を用いてカプセルヘッダに対応するＩＰカプセルヘッダ及び出力側ＭＡＣアドレスを出力側カプセル番号（３２６）から生成する。こうして生成されたＩＰカプセルヘッダ、出力側ＭＡＣアドレスとＩＰパケットはカプセルレイヤ送信処理部（１７６）でカプセル化処理され、物理レイヤ送信処理部（１７５）を介してＩＳＰ１のネットワークへと送信される。

【００５２】図１９にヘッダ生成テーブルの構成を示す。出力側カプセル番号をキーとして出力側ＩＰカプセルヘッダ及び出力側ＭＡＣアドレスを出力する構成となっている。

【００５３】以上インターワークルータ装置の一構成例を示した。本実施例では、入力側、出力側それぞれの処理に内部で統一された入力側ＶＰＮ番号（３２０）及び出力側カプセル番号（３２６）を用いた例を示した。但し、ルート検索・ＶＰＮテーブルの入力キーを入力側カプセルヘッダにしてもよいし、出力として直接出力側カプセルヘッダを生成してもよい。

【００５４】また、本実施例で示したテーブルは論理的なテーブルであり、テーブル検索方法として、ツリー構造に代表される検索アルゴリズムを用いてアドレスを出し、所望の出力を得る方式を採用してもよいし、ＣＡＭを使った構成や、テーブルを逐次検索していく方式を採用してもよい。

【００５５】図２３に本実施例のテーブルの設定のための、ＮＭＳから装置に指示を出すインターフェースであり、エージェントが制御部５０に搭載される、ＭＩＢ（Management Information Base）構成の一実施例を示す。入力カプセルヘッダEntry（５００）は図１３に示した受信側VPNテーブルを設定するためのＭＩＢである。同様にＶＰＮクロスコネクトEntry（５０１）は図１７に示したルート検索・ＶＰＮテーブル（１８２）を設定するためのＭＩＢである。同様に出力側カプセルヘッダEntry（５０２）はヘッダ生成テーブルの１構成例である。これらのＭＩＢに設定された情報は、ＮＭＳから制御部（５０）に対して設定され、制御部（５０）がインターワークルータ内各部にテーブル設定する。

【００５６】ここまでにＶＰＮのインターワークについて装置構成を中心に説明してきた。図２０から図２２を用いて、インターワークルータのネットワーク内での適用例を説明する。

【００５７】図２０は２つのＩＳＰがそれぞれの所有する２つのインターワークルータを介して接続される例を示す。２つのインターワークルータの間はカプセル化（１０３ｂ）によりそれぞれのＶＰＮを識別する構成になっている。そしてそれぞれのインターワークルータ（１０ａ、１０ｂ）では、図１９までに説明したとおり、カプセルヘッダ（１０３ａ、１０３ｂ、１０３ｃ）とＩＰアドレスの組によりルーティング処理を行う。

【００５８】図２１は２つのＩＳＰがそれぞれの所有するインターワークルータを持ち、レイヤ３処理を行うＩＸを介して接続される例である。それぞれのインターワークルータとＩＸの間はカプセル化（１０３ｂ）によりそれぞれのＶＰＮを識別する構成になっている。インターワークルータ（１０ａ）、ＩＸ（１０ｃ）及びインターワークルータ（１０ｂ）では、図１９までに説明したとおり、カプセルヘッダ（１０３ａ、１０３ｂ、１０３ｃ）とＩＰアドレスの組によりフォワーディング処理を行う。

【００５９】図２２は２つのＩＳＰはそれぞれのインターワークルータを持ち、２つのＩＳＰが、ＩＸを介して接続される例を示す。ここで、ＩＸはレイヤ３処理を行わないレイヤ２装置で構成されている。この場合もそれぞれのインターワークルータとＩＸの間はカプセル化（１０３ｂ）によりそれぞれのＶＰＮを識別する構成になっている。インターワークルータ（１０ａ）とインターワークルータ（１０ｂ）では、図１９までに説明したとおり、カプセルヘッダ（１０３ａ、１０３ｂ、１０３ｃ）とＩＰアドレスの組によりフォワーディング処理を行う。ＩＸはレイヤ２フォワーディングにより転送を行う。

【００６０】なお、本発明では複数ＩＳＰ間のＶＰＮの接続方式について説明したが、同一ＩＳＰ内に複数のカプセル化エリアが存在する場合にも、同一のノード構成でＶＰＮを接続することが必要である。その場合でも、本発明で説明した方式により、ＶＰＮを接続することができる。

【００６１】

【発明の効果】本発明により複数ＩＳＰ間にまたがるＶＰＮ網を構築することができる。また複数のＶＰＮネットワーク間でＱｏＳ情報をインターワークすることができる。

【図面の簡単な説明】

【図１】本発明によるインターワークルータ動作の概念図である。

【図２】従来のルータを用いた場合における複数のＩＳＰ間のインターワーク方式を説明した図である。

【図３】本発明によるインターワークルータの動作をプロトコルスタックを用いて説明した図である。

【図４】従来のルータによるＩＳＰインターワーク処理方式を説明するフローチャートである。

【図５】本発明によるインターワークルータの動作を説明するフローチャートである。

【図６】本発明によるインターワークルータの動作を説明するフローチャートである。

【図７】本発明によるＭＰＬＳ網とＩＰカプセル化網の接続形態をプロトコルスタックを用いて説明した図である。

【図８】ＲＦＣ１４８３によるＩＰパケットのＡＴＭセル化を説明する図である。

【図９】ＲＦＣ７９１によるＩＰパケットフォーマットを説明する図である。

【図１０】ＲＦＣ１８５３によるＩＰトンネルパケットの構成を説明する図である。

【図１１】本発明によるインターワークルータの１構成例を説明する図である。

【図１２】本発明によるインターワークルータの下位レイヤ処理部の１構成例を説明する図である。

【図１３】本発明による下位レイヤ処理部における受信側ＶＰＮ番号テーブルの構成例を説明する図である。

【図１４】本発明によるインターワークルータの下位レイヤ処理部の１構成例を説明する図である。

【図１５】本発明による下位レイヤ処理部における受信側ＶＰＮ番号テーブルの構成例を説明する図である。

【図１６】本発明によるインターワークルータのパケットレイヤ処理部の１構成例を説明する図である。

【図１７】本発明によるパケットレイヤ処理部におけるルート検索ＶＰＮテーブルの構成例を説明する図である。

【図１８】本発明による下位レイヤ処理部におけるヘッダ生成テーブルの構成例を説明する図である。

【図１９】本発明による下位レイヤ処理部におけるヘッダ生成テーブルの構成例を説明する図である。

【図２０】本発明によるインターワークルータの網内での１適用例を説明する図である。

【図２１】本発明によるインターワークルータの網内での１適用例を説明する図である。

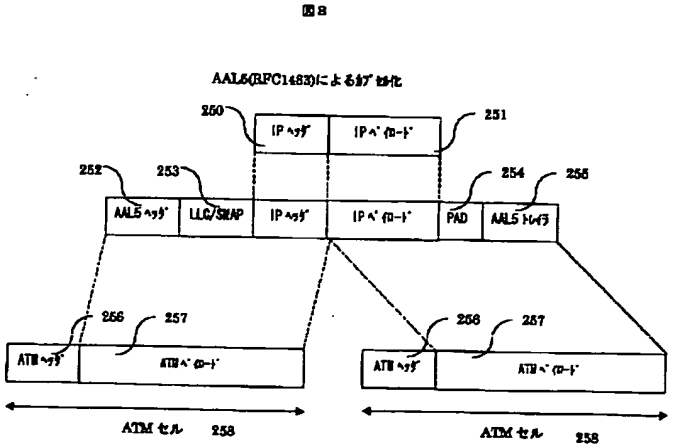
【図２２】本発明によるインターワークルータの網内での１適用例を説明する図である。

【図２３】本実施例のテーブルの設定のための、ＮＭＳから装置に指示を出すインターフェースである。

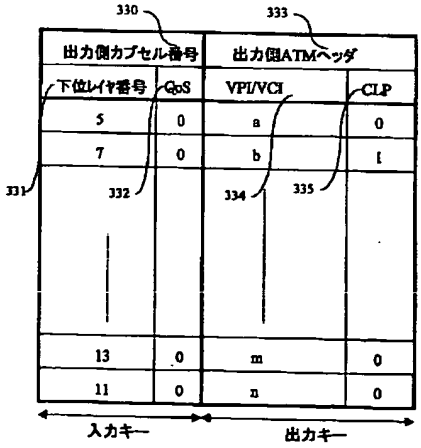
【符号の説明】

２…ＩＳＰ網、３…エッジノード、１０…インターワークルータ装置、５０…制御部、５１…コアスイッチ、５２…パケットレイヤ処理部、５３…下位レイヤ処理部（ＡＴＭ）、５４…下位レイヤ処理部（ＩＰカプセル）、１５２…ＶＰＮ番号付与部、１５３…受信側ＶＰＮ番号テーブル、１５７…ＡＴＭヘッダ決定部、１５８…ヘッダ生成テーブル、１７２…ＶＰＮ番号付与部、１７３…受信側ＶＰＮ番号テーブル、１７７…カプセルヘッダ決定部、１７８…ヘッダ生成テーブル。

【図８】

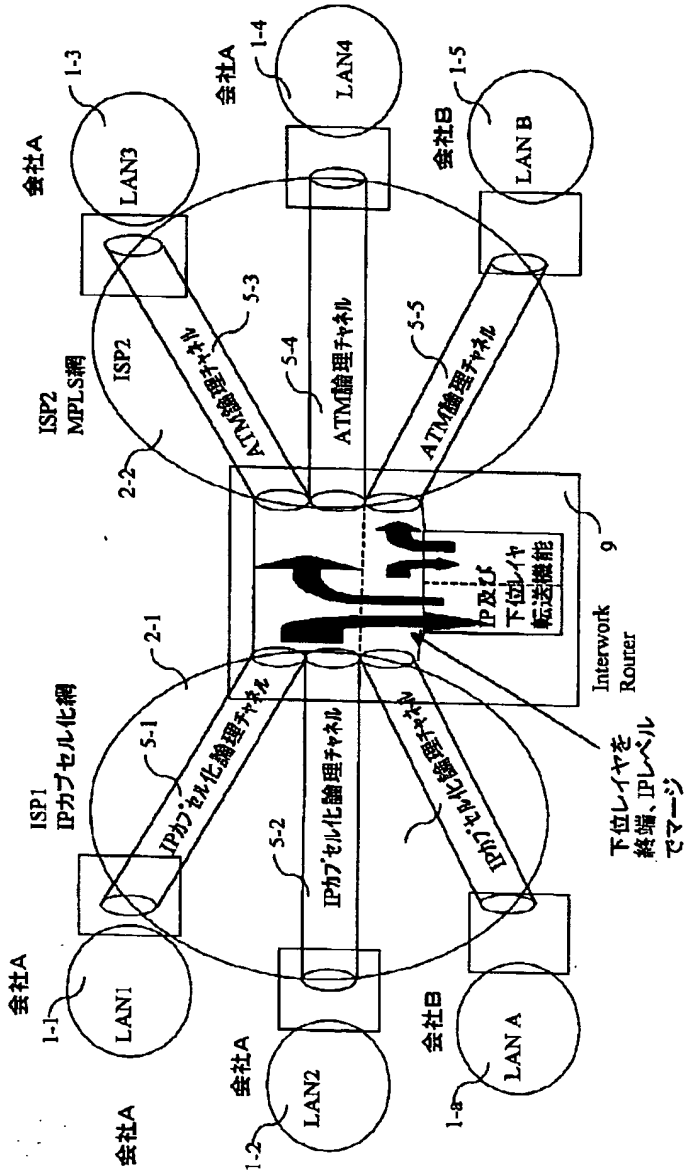


【図１８】



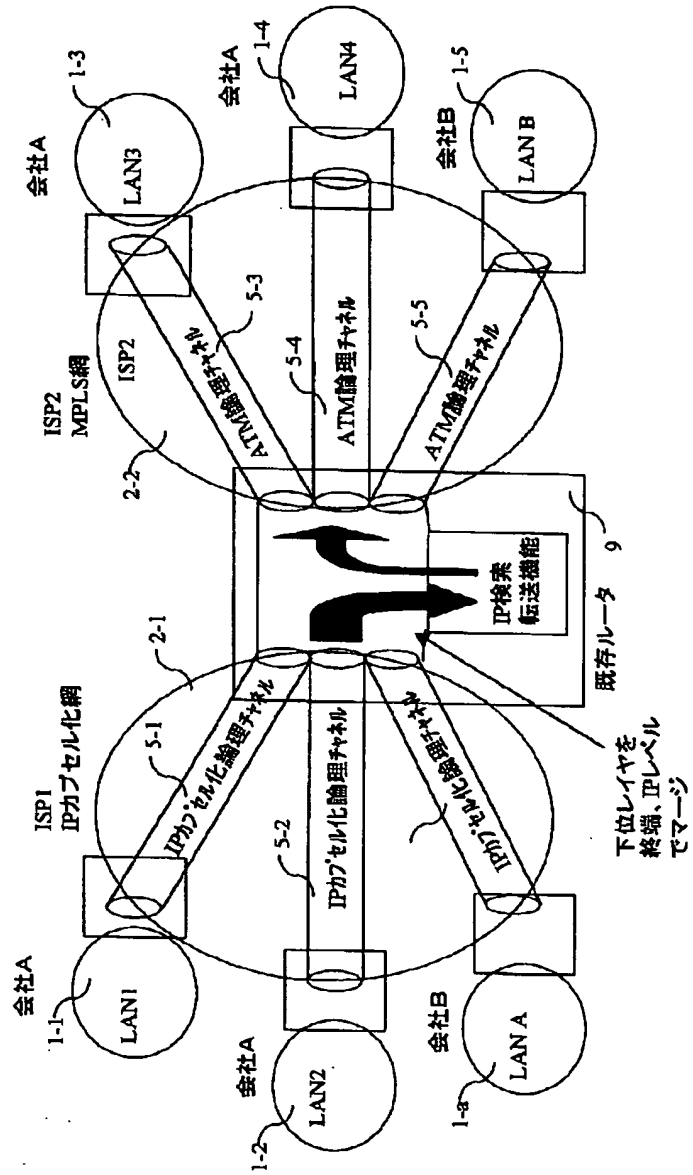
【図１】

図1


会社A
LAN1
1-1
会社A
LAN2
1-2
会社A
LAN3
1-3
会社A
LAN4
1-4
会社B
LAN A
1-a
会社B
LAN B
1-5
ISP1
IPカプセル化網
ISP2
MPLS網
ISP2
2-1
2-2
IPカプセル化論理チャネル
5-1
IPカプセル化論理チャネル
5-2
ATM論理チャネル
5-3
ATM論理チャネル
5-4
ATM論理チャネル
5-5
IP及び
下位レイヤ
転送機能
9
Interwork
Rourer
下位レイヤを
終端、IPレベル
でマージ

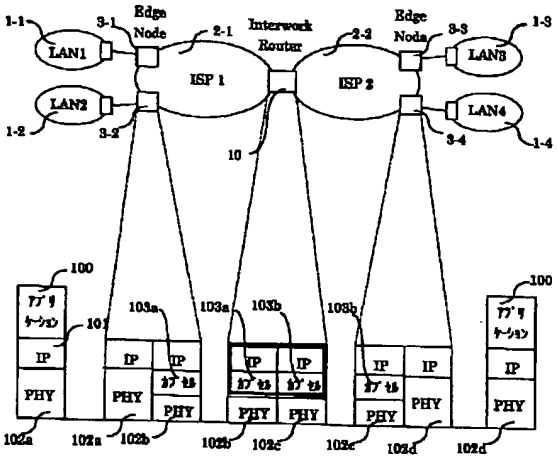
【図２】

図2


会社A
LAN1
1-1
会社A
LAN2
1-2
会社A
LAN3
1-3
会社A
LAN4
1-4
会社B
LAN B
1-5
会社B
LAN A
1-a
ISP1
IPカプセル化網
ISP2
MPLS網
ISP2
2-1
2-2
IPカプセル化論理チャネル
5-1
IPカプセル化論理チャネル
5-2
ATM論理チャネル
5-3
ATM論理チャネル
5-4
ATM論理チャネル
5-5
IP検索
転送機能
既存ルータ
9
下位レイヤを
終端、IPレベル
でマージ

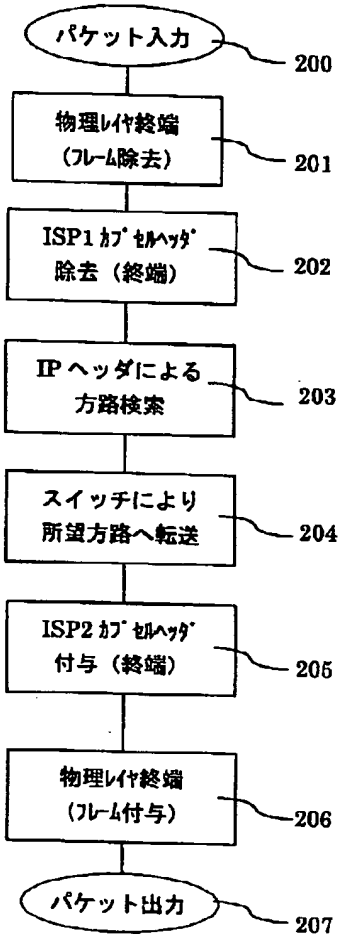
【図３】

図３



【図４】

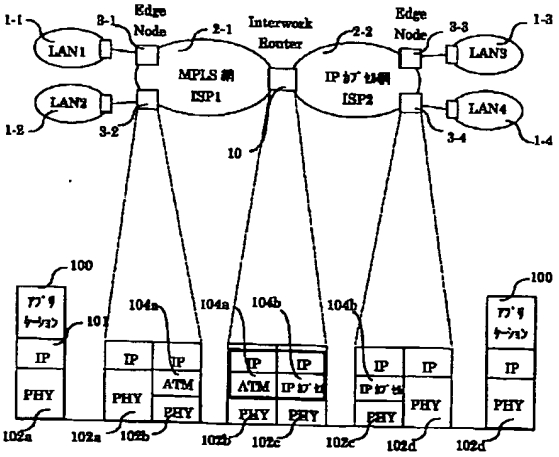
図４



ルータの処理の流れ（従来例）

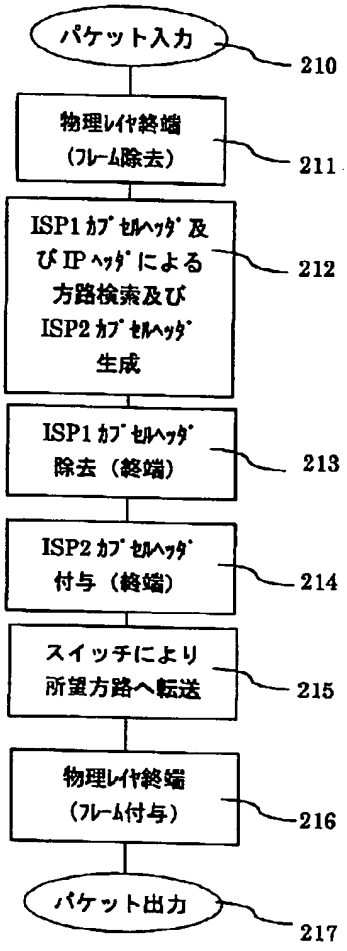
【図７】

図７



【図５】

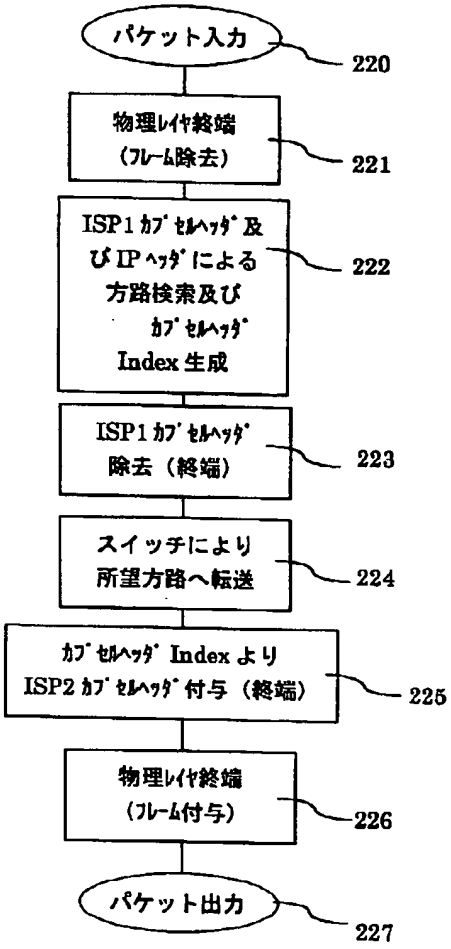
図５



インターワークルータの処理の流れ（本発明）

【図６】

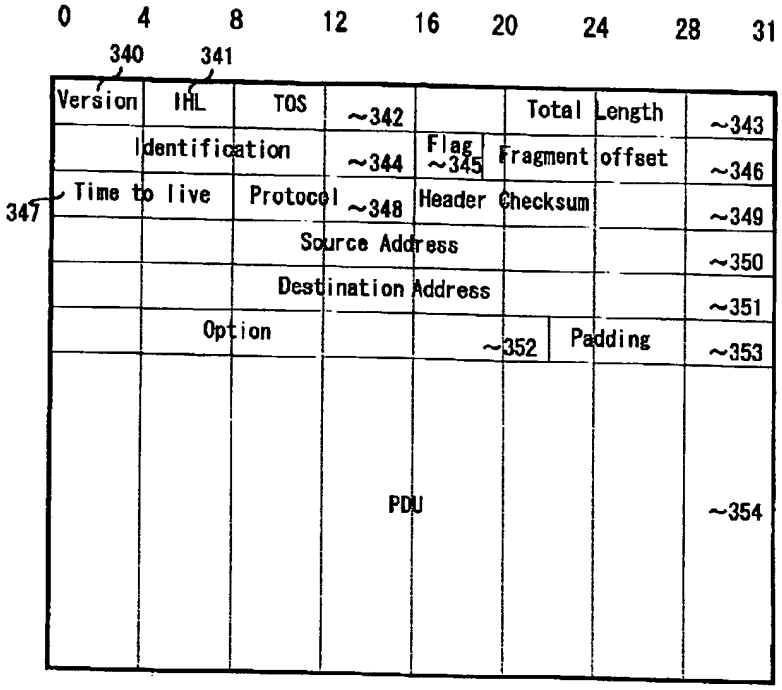
図６



インターワークルータの処理の流れ（本発明）

【図９】

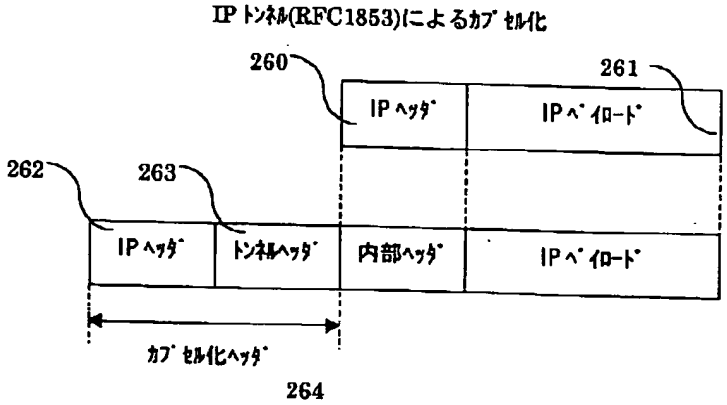
図９



IPv4 フレームフォーマット

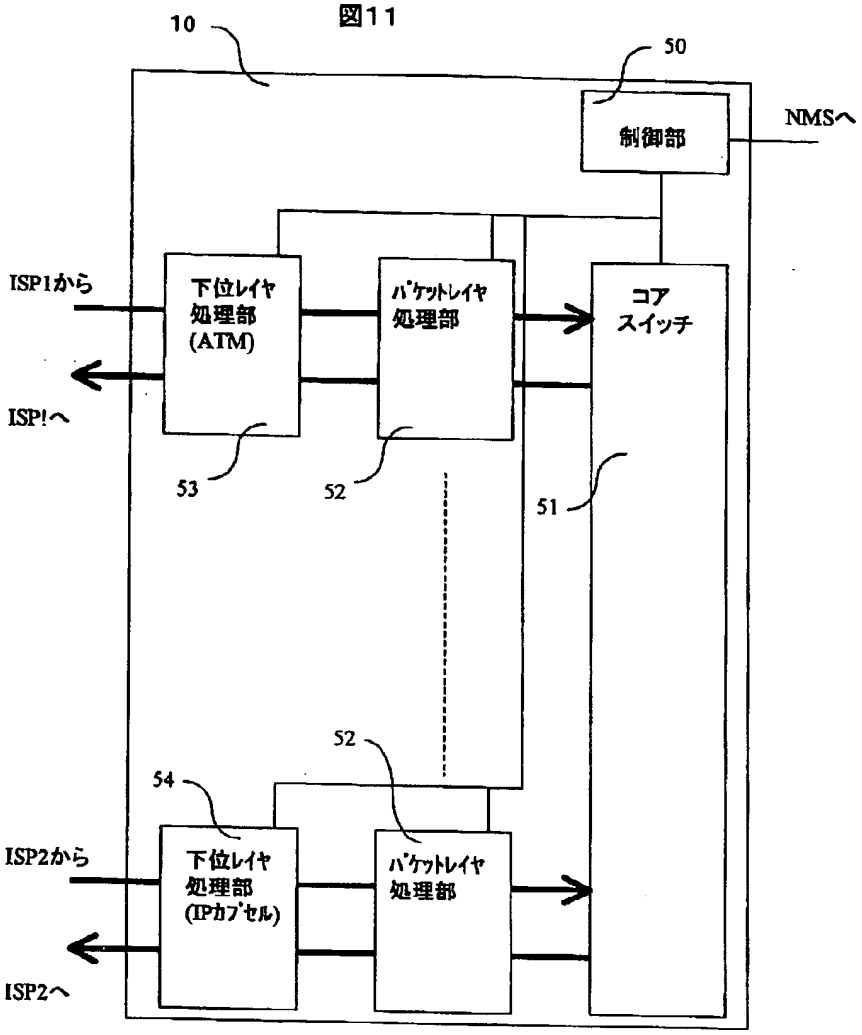
【図１０】

図１０



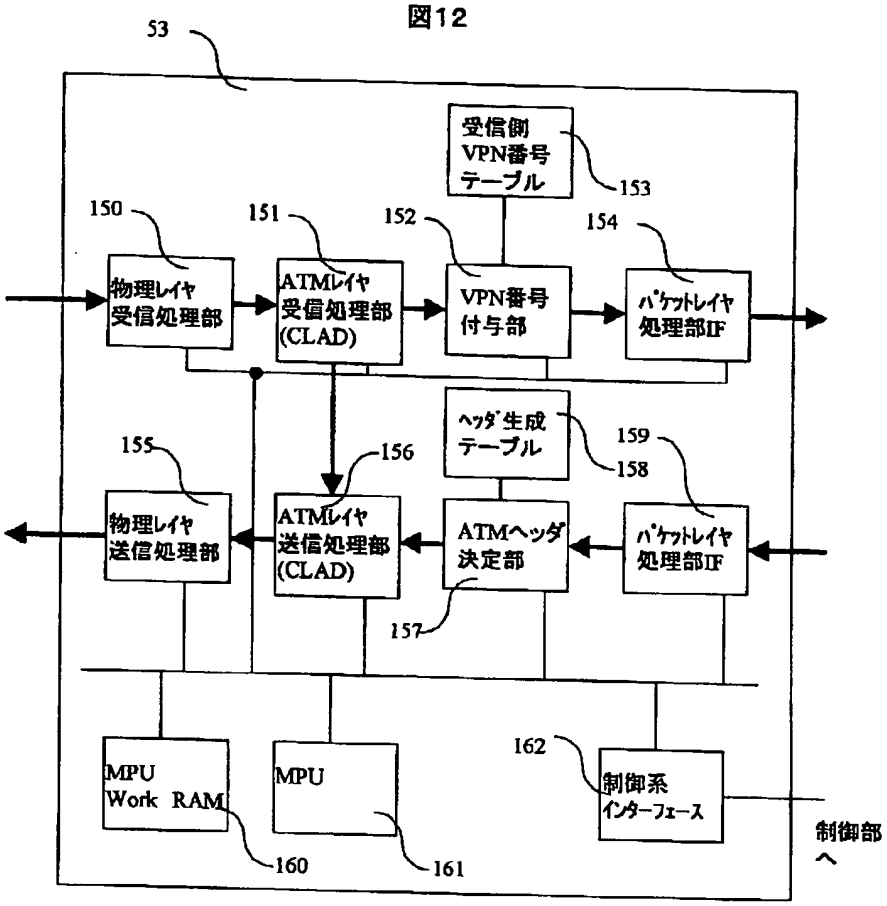
【図１１】

図11


10
50
制御部
NMSへ
ISP1から
下位レイヤ
処理部
(ATM)
パケットレイヤ
処理部
コア
スイッチ
ISP1へ
53
52
51
52
54
ISP2から
下位レイヤ
処理部
(IPカプセル)
パケットレイヤ
処理部
ISP2へ

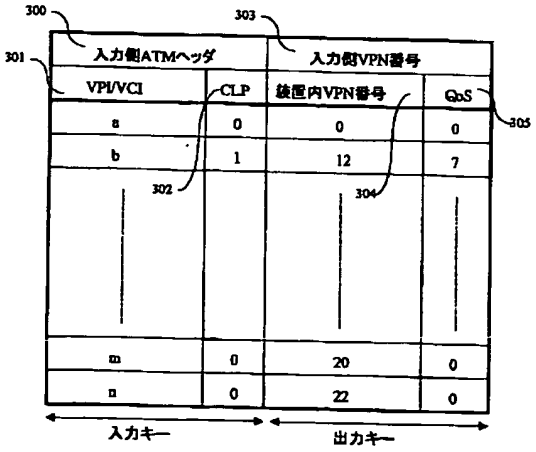
【図１２】

図12



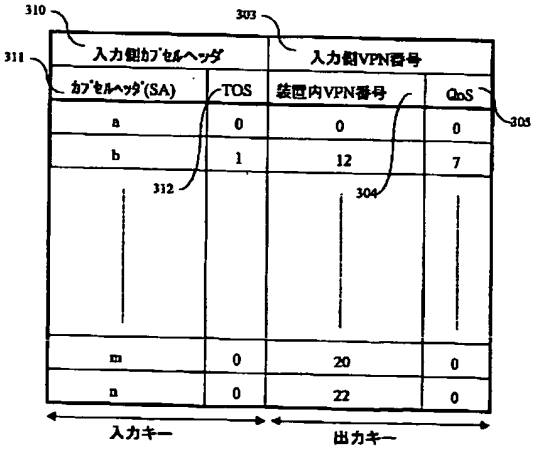
【図１３】

図13



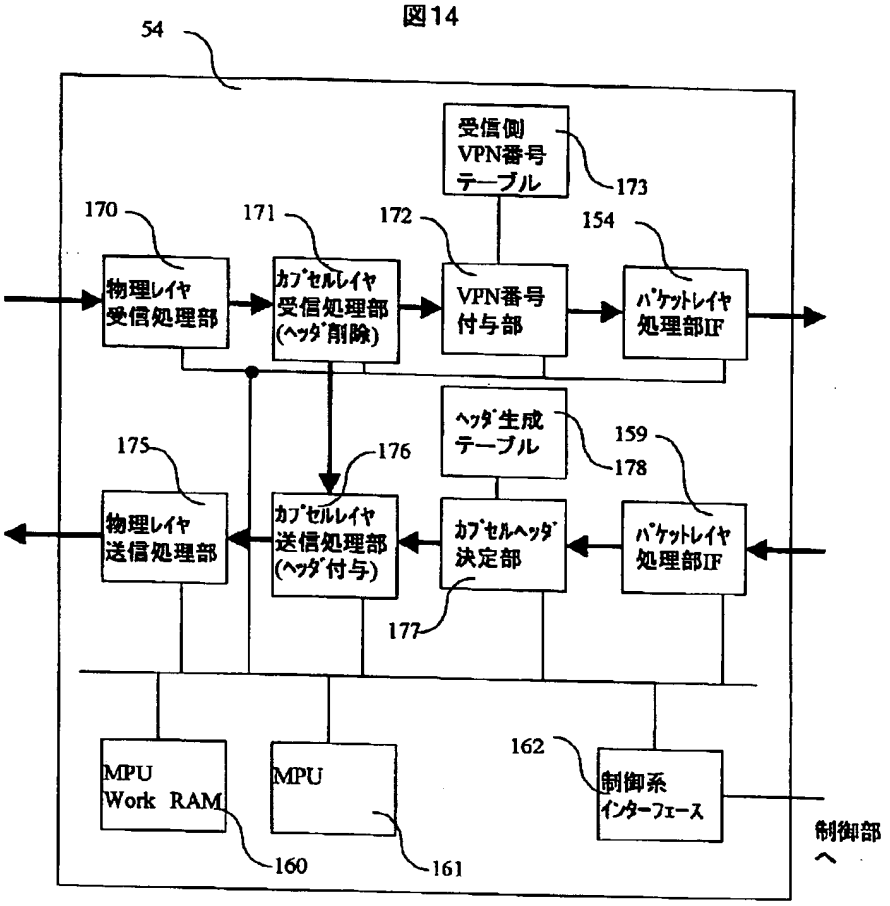
【図１５】

図15



【図１４】

図14



【図１７】

図17

320	321	323		325	326	
入力側VPN番号		IPヘッダ		出力方路番号	出力側ｶﾌﾟｾﾙ番号	
装置内VPN番号	QoS	Destination Address			ｶﾌﾟｾﾙ番号	QoS
1	0	A.a.a.a		15	5	0
1	0	b.a.a.a		10	7	0
322		324		327	328	
n	0	b.a.a.a		8	13	0
n	0.	c.a.a.a		2	11	0

入力キー　出力キー

【図１９】

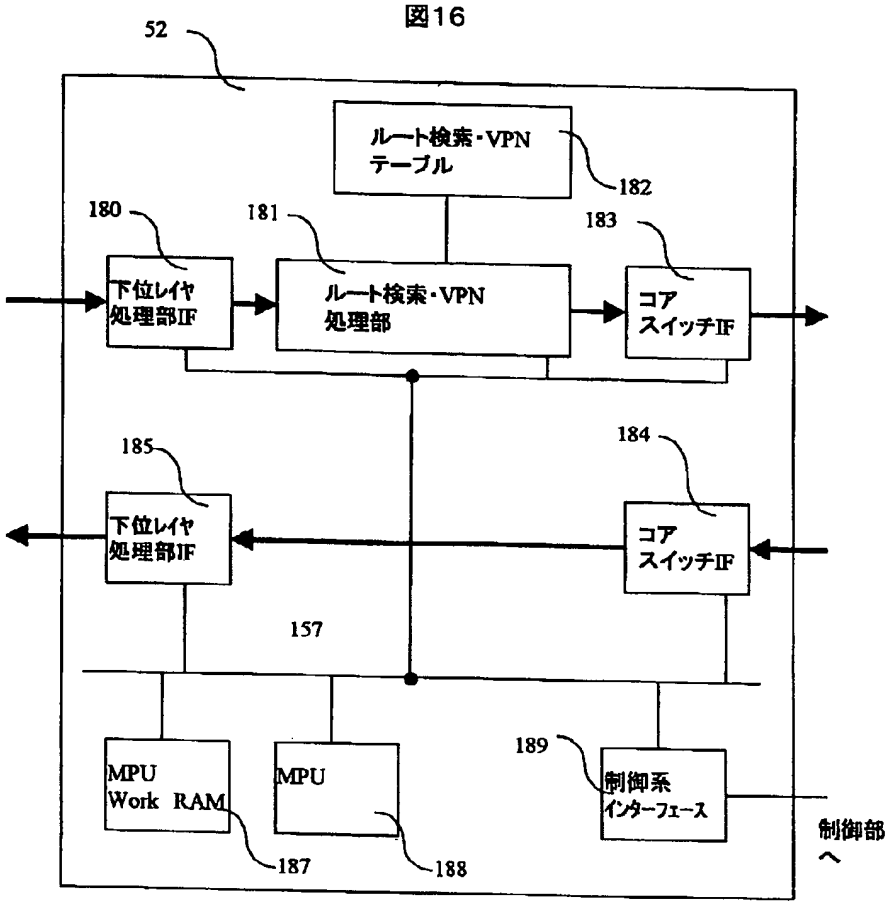
図19

340		343	345
出力側ｶﾌﾟｾﾙ番号		出力側IPｶﾌﾟｾﾙﾍｯﾀﾞ	出力側MACｱﾄﾞﾚｽ
下位レイヤ番号	QoS	IPｶﾌﾟｾﾙﾍｯﾀﾞ	
5	0	a	あ
7	0	b	う
341	342	344	
13	0	m	た
11	0	n	い

入力キー　出力キー

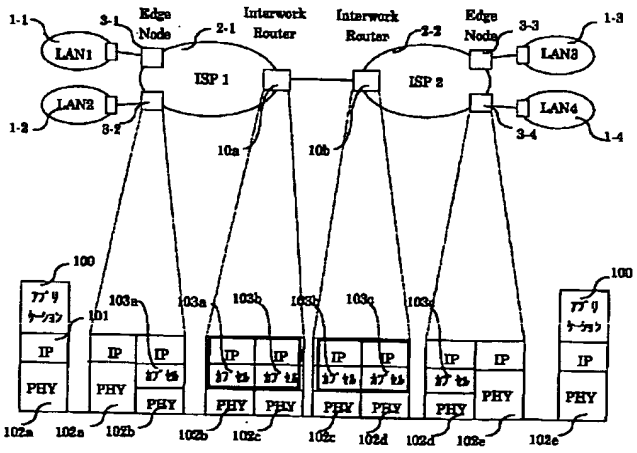
【図１６】

図16



【図２０】

図20



【図２１】

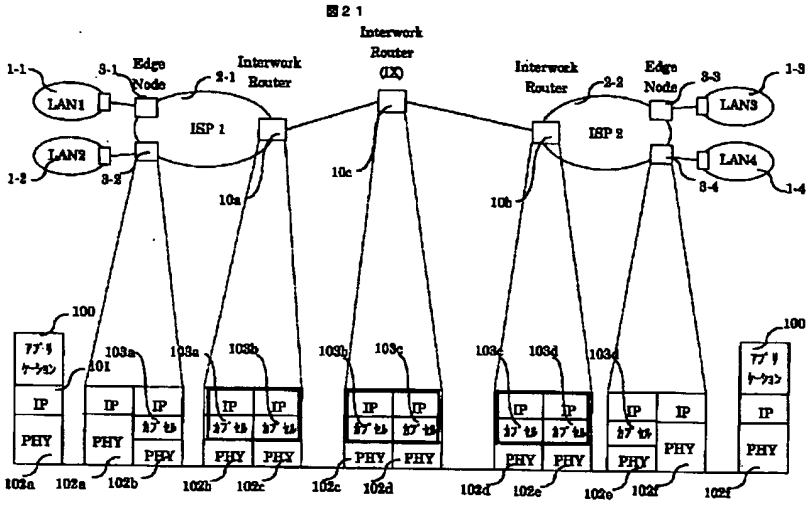


図２１
Interwork Router (IX)
Edge Node
Interwork Router
ISP 1
ISP 2
LAN1
LAN2
LAN3
LAN4
IP
PHY
アプリケーション

【図２２】

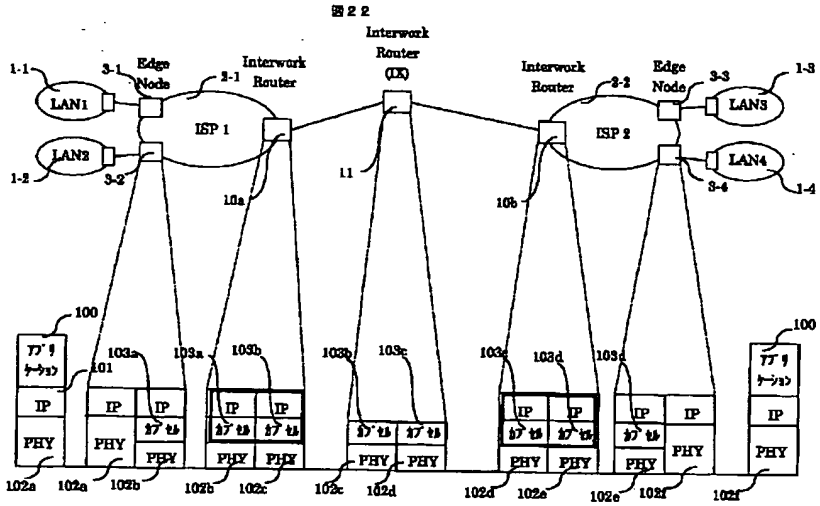
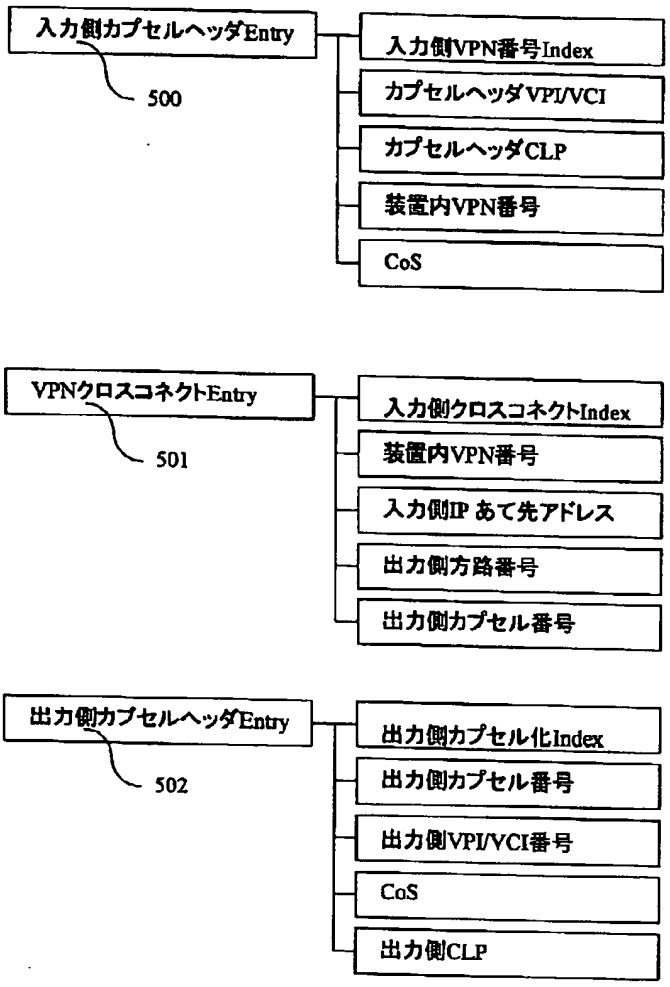


図２２
Interwork Router (IX)
Edge Node
Interwork Router
ISP 1
ISP 2
LAN1
LAN2
LAN3
LAN4
IP
PHY
アプリケーション

【図２３】

図23



フロントページの続き

(72)発明者 若山 浩二
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内

(72)発明者 田辺 史朗
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内

(72)発明者 遠藤 昇
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内

Fターム(参考) 5K030 GA11 HA10 HC13 HD03 HD06
HD09 JA05 KA05 KA13
5K033 AA09 CB08 CC01 DA05 DB12
DB14 DB18
9A001 BB06 CC02 CC06 CC08 JJ12
JJ25 KK56

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.